

DOCKET NO.: 255234US6PCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Satoshi KITANI, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP03/16937

INTERNATIONAL FILING DATE: December 26, 2003

FOR: SIGNAL PROCESSING SYSTEM, RECORDING METHOD, PROGRAM, RECORDING  
MEDIUM, REPRODUCING APPARATUS, AND INFORMATION PROCESSING APPARATUS

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119**  
**AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents  
Alexandria, Virginia 22313

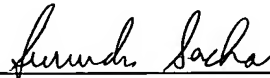
Sir:

In the matter of the above-identified application for patent, notice is hereby given that  
the applicant claims as priority:

<b><u>COUNTRY</u></b>	<b><u>APPLICATION NO</u></b>	<b><u>DAY/MONTH/YEAR</u></b>
Japan	2003-006916	15 January 2003

Certified copies of the corresponding Convention application(s) were submitted to the  
International Bureau in PCT Application No. PCT/JP03/16937. Receipt of the certified  
copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been  
acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



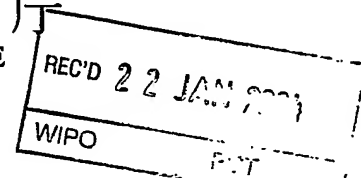
\_\_\_\_\_  
Gregory J. Maier  
Attorney of Record  
Registration No. 25,599  
Surinder Sachar  
Registration No. 34,423

Customer Number

**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

日本国特許庁  
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 1月15日  
Date of Application:

出願番号 特願2003-006916  
Application Number:  
[ST. 10/C]: [JP 2003-006916]

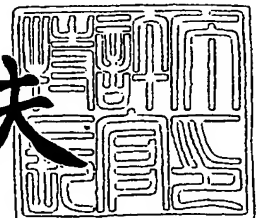
出願人 ソニー株式会社  
Applicant(s):

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2003年11月 7日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0290810006

【提出日】 平成15年 1月15日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 H04N 5/85

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 木谷 聡

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 村松 克美

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100082762

【弁理士】

【氏名又は名称】 杉浦 正知

【電話番号】 03-3980-0339

【選任した代理人】

【識別番号】 100120640

【弁理士】

【氏名又は名称】 森 幸一

【手数料の表示】

【予納台帳番号】 043812

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0201252

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 信号処理システム、記録方法、プログラム、記録媒体、再生装置および情報処理装置

【特許請求の範囲】

【請求項 1】 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達手段を介して相互認証接続される情報処理装置とを備える信号処理システムであって、

上記再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第 1 の送信手段と、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第 2 の送信手段とを有し、

上記情報処理装置は、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化手段と、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録手段とを有する信号処理システム。

【請求項 2】 請求項 1 において、

上記再生装置は、

乱数を生成する乱数生成手段を有し、

上記中間鍵情報は、

上記乱数生成手段により生成された乱数である信号処理システム。

【請求項 3】 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達手段を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録する記録方法であって、

上記再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第1の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第2の送信ステップとを有し、

上記情報処理装置は、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを有する記録方法。

【請求項4】 請求項3において、

上記再生装置は、

乱数を生成する乱数生成ステップを有し、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数である記録方法。

【請求項5】 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達手段を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録するプログラムであって、

上記再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第1の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第2の送信ステップとを行わせ、

上記情報処理装置に、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを行わせるプログラム。

【請求項 6】 請求項 5 において、

上記再生装置に、

乱数を生成する乱数生成ステップを行わせ、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数であるプログラム。

【請求項 7】 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達手段を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録するプログラムを格納した記録媒体であって、

上記再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第 1 の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第 2 の送信ステップを行わせ、

上記情報処理装置に、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記

記録媒体に記録する記録ステップとを行わせるプログラムを格納した記録媒体。

【請求項 8】 請求項 7 において、

上記再生装置に、

乱数を生成する乱数生成ステップを行わせ、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数であるプログラムを格納した記録媒体。

【請求項 9】 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出し、伝達手段を介して情報処理装置と接続される再生装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第 1 の送信手段と、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第 2 の送信手段とを有し、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化手段と、暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録手段とを有する上記情報処理装置と相互認証接続される再生装置。

【請求項 10】 請求項 9 において、

乱数を生成する乱数生成手段を有し、

上記中間鍵情報は、

上記乱数生成手段により生成された乱数である再生装置。

【請求項 11】 記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と伝達手段を介して接続される情報処理装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第 1 の送信手段と、上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装



置へ送る第2の送信手段とを有する上記再生装置と伝達手段を介して相互認証接続され、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化手段と、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報を上記記録媒体に記録する記録手段とを有する情報処理装置。

【請求項12】 請求項11において、

上記再生装置は、

乱数を生成する乱数生成手段を有し、

上記中間鍵情報は、

上記乱数生成手段により生成された乱数である情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される信号処理システム、記録方法、プログラム、記録媒体、再生装置および情報処理装置に関する。

【0002】

【従来の技術】

近年開発されたDVD (Digital Versatile Disc またはDigital Video Disc) 等の記録媒体では、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

【0003】

DVD-Videoでは、コピープロテクション技術としてCSS (Content Scramb

ling System)が採用されている。CSSは、DVD-ROMメディアに対する適用のみが認可されており、DVD-R、DVD-RW、DVD+R、DVD+RW等の記録型DVDでのCSSの利用がCSS契約によって禁止されている。したがって、CSS方式で著作権保護されたDVD-Videoの内容を記録型DVDへのまるごとコピー（ビットバイビットコピー）することは、CSS契約上では、認められた行為ではない。

#### 【0004】

しかしながら、CSSの暗号方式が破られる事態が発生した。CSSの暗号化を解除してDVD-Videoの内容を簡単にハードディスクにコピーすることを可能とする「DeCSS」と呼ばれるソフトウェアがインターネット上で配布された。「DeCSS」が出現した背景には、本来耐タンパー化が義務付けられているはずのCSS復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にCSSアルゴリズム全体が解読された経緯がある。

#### 【0005】

CSSの後に、DVD-Audio等のDVD-ROMの著作権保護技術であるCPPM(Content Protection for Pre-Recorded Media)、並びに記録型DVD、メモリカードに関する著作権保護技術CPRM(Content Protection for Recordable Media)が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、また、データをまるごとコピーしても再生を制限できる特徴を有している。DVDに関する著作権保護の方法に関しては、下記の非特許文献1に説明され、CPRMは、ライセンス管理者である米4C Entity, LLCが配布する下記の資料（非特許文献2）に説明されている。

#### 【0006】

##### 【非特許文献1】

山田, 「DVDを起点に著作権保護空間を広げる」, 日経エレクトロニクス 2001.8.13, p.143-153

#### 【0007】

## 【非特許文献2】

”Content Protection for Recordable Media Specification DVD Book”、インターネット<URL：<http://www.4Centity.com/>>

## 【0008】

## 【発明が解決しようとする課題】

パーソナルコンピュータ（以下、適宜PCと略す）環境下では、PCとドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。また、アプリケーションソフトウェアがリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

## 【0009】

著作権保護技術をPC上で実行されるアプリケーションプログラムへ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がなく、その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。CSSの場合は、結果としてその著作権保護技術が破られてしまった。さらに、CSSの後に提案されたCPRMおよび記録型DVDに関する著作権保護技術CPRMにおいても、既に破られているCSSに新たな機能を加えたものであり、また、著作権保護技術に関わるアルゴリズムは、大部分がPCでの実装に依存するものであり、コンテンツプロテクションの機能が十分に強いものと言えない問題があった。すなわち、アプリケーションソフトウェアなどのリバースエンジニアリングによって、著作権保護技術に関わる秘密情報の解析により暗号方式が破られ、ディスクからのデータとしてPCがそのまま読み出した暗号化コンテンツが「DeCSS」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を招くことで、著作権保護が機能しなくなるという危険性があった。

## 【0010】

したがって、この発明の目的は、PC環境下でも著作権保護技術の安全性を確保することができる信号処理システム、記録方法、プログラム、記録媒体、再生装置および情報処理装置を提供することにある。

#### 【0011】

##### 【課題を解決するための手段】

上述した課題を解決するために、請求項1の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達手段を介して相互認証接続される情報処理装置とを備える信号処理システムであって、再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

中間鍵情報を伝達手段を介して情報処理装置へ送る第1の送信手段と、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第2の送信手段とを有し、

情報処理装置は、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化手段と、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録手段とを有する信号処理システムである。

#### 【0012】

請求項3の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達手段を介して相互認証接続される情報処理装置とが、記録媒体に情報を記録する記録方法であって、

再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達手段を介して情報処理装置へ送る第1の送信ステップと、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第2の送信ステップとを有し、

情報処理装置は、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを有する記録方法である。

### 【0013】

請求項5の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達手段を介して相互認証接続される情報処理装置とが、記録媒体に情報を記録するプログラムであって、

再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達手段を介して情報処理装置へ送る第1の送信ステップと、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第2の送信ステップとを行わせ、

情報処理装置に、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを行わせるプログラムである。

### 【0014】

請求項7の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達手段を介して相互認証接続される情報処

理装置とが、記録媒体に情報を記録するプログラムを格納した記録媒体であって

、

再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達手段を介して情報処理装置へ送る第1の送信ステップと、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第2の送信ステップを行わせ、

情報処理装置に、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを行わせるプログラムを格納した記録媒体である。

#### 【0015】

請求項9の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出し、伝達手段を介して情報処理装置と接続される再生装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

中間鍵情報を伝達手段を介して情報処理装置へ送る第1の送信手段と、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第2の送信手段とを有し、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化手段と、暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録手段とを有する情報処理装置と相互認証接続される再生装置である。

#### 【0016】

請求項 11 の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と伝達手段を介して接続される情報処理装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、中間鍵情報を伝達手段を介して情報処理装置へ送る第 1 の送信手段と、コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第 2 の送信手段とを有する再生装置と伝達手段を介して相互認証接続され、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化手段と、

暗号化されたコンテンツ情報および暗号化された中間鍵情報を記録媒体に記録する記録手段とを有する情報処理装置である。

#### 【0017】

この発明では、再生装置側でコンテンツキーを生成し、情報処理装置側でコンテンツキーによってコンテンツを暗号化している。このように著作権保護のための鍵情報の生成を再生装置で行うので、ハードウェア構成でコンテンツキーを生成することが可能となり、耐タンパー性を高めることができる。また、再生装置において、乱数を生成し、乱数を中間鍵とするので、再生装置において、真正乱数またはそれに近い乱数をハードウェア例えば LSI によって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。このように、この発明では、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

#### 【0018】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えば LSI によって生成できるので、PC 内でソフトウ

ェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

#### 【0019】

##### 【発明の実施の形態】

この発明の一実施形態の説明に先立って、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

#### 【0020】

記録媒体：メディア例えばディスク、再生装置：ドライブ、情報処理装置：ホスト、伝達手段：ドライバ－ホストインターフェース、信号処理システム：メディアを再生するドライブとホストとがドライバ－ホストインターフェースを介して接続されるシステムである。第1の送信手段：ドライブ側からセッションキーを共通鍵とした共通鍵暗号方式で情報をホスト側に送る手段、第2の送信手段：逆にホスト側からセッションキーを共通鍵として情報をドライブ側に送る手段のことである。

#### 【0021】

コンテンツ情報：メディアに記録されている情報または記録すべき情報をコンテンツ情報としている。記録媒体固有の情報：メディアIDである。乱数を生成する乱数生成手段：乱数発生器（RNG：Random Number Generator）である。記録媒体固有の鍵情報：メディアユニークキー、中間鍵情報：タイトルキーである。コンテンツ情報暗号化鍵：コンテンツキー（記録時に使われるコンテンツキーをコンテンツ情報暗号化鍵とし、再生時に使われるコンテンツキーをコンテンツ情報復号鍵としている。）

#### 【0022】

次に、この発明の理解の容易のために、最初に図1を参照して著作権保護技術例えばDVD用CPRMのアーキテクチャについて説明する。図1において、参照符号1が例えばCPRM規格に準拠したDVD-R/RW、DVD-RAM等の記録型DVDメディアを示し、参照符号2が例えばCPRM規格に準拠したレ



コードを示し、参照符号 3 が例えば CPRM 規格に準拠したプレーヤを示す。レコーダ 2 およびプレーヤ 3 は、機器またはアプリケーションソフトウェアである。

### 【0023】

未記録ディスクの状態において、DVD メディア 1 の最内周側のリードインエリアの BCA (Burst Cutting Area) または NB CA (Narrow Burst Cutting Area) と称されるエリアには、メディア ID 1 1 が記録され、リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック (以下、MKB と適宜略す) 1 2 が予め記録されている。メディア ID 1 1 は、個々のメディア単位例えばディスク 1 枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディア ID 1 1 は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロック MKB は、メディアキーの導出、並びに機器のリボケーション (無効化) を実現するための鍵束である。これらのメディア ID およびメディアキーブロックは、記録媒体固有の第 1 の情報である。

### 【0024】

ディスク 1 の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ 1 3 が記録される。暗号化方式としては、C 2 (Cryptomeria Cipherng) が使用される。

### 【0025】

DVD メディア 1 には、暗号化タイトルキー 1 4 および CCI (Copy Control Information) 1 5 が記録される。暗号化タイトルキー 1 4 は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。CCI は、コピーノーマ、コピーワンス、コピーフリー等のコピー制御情報である。

### 【0026】

レコーダ 2 は、デバイスキー 2 1、プロセス MKB 2 2、C 2 \_\_G 2 3、乱数発生器 2 4、C 2 \_\_E 2 5、C 2 \_\_G 2 6 および C 2 \_\_E C B C 2 7 の構成要素を有する。プレーヤ 3 は、デバイスキー 3 1、プロセス MKB 3 2、C 2 \_\_G 3

3、C2\_\_D35、C2\_\_G36およびC2\_\_DCBC37の構成要素を有する。C2\_\_G23および33は、それぞれメディアIDとメディアキーとからメディアユニークキーを演算するブロックである。C2\_\_G26および36は、それぞれCCIとタイトルキーとからコンテンツキーを演算するブロックである。

#### 【0027】

デバイスキー21、31は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。DVDメディア1から再生されたMKB12とデバイスキー21とがプロセスMKB22において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ2におけるのと同様に、プレーヤ3においても、MKB12とデバイスキー31とがプロセスMKB32において演算され、リボケーションされたかどうかの判別がなされる。

#### 【0028】

さらに、プロセスMKB22、32のそれぞれにおいて、MKB12とデバイスキー21、31からメディアキーが算出される。MKB12の中にレコーダ2またはプレーヤ3のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ2またはプレーヤ3が正当なものでないと判断される。すなわち、そのようなレコーダ2またはプレーヤ3がリボケーションされる。

#### 【0029】

C2\_\_G23、33は、それぞれ、メディアキーとメディアIDとを演算し、メディアユニークキーを導出する処理である。

#### 【0030】

乱数発生器(RNG:Random Number Generator)24は、タイトルキーの生成に利用される。乱数発生器24からのタイトルキーがC2\_\_E25に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー14がDVDメディア1に記録される。

## 【0031】

プレーヤ3では、DVDメディア1から再生された暗号化タイトルキー14とメディアユニークキーとがC2\_\_D35に供給され、暗号化タイトルキーがメディアユニークキーで復号され、タイトルキーが得られる。

## 【0032】

レコーダ2においては、CCIとタイトルキーとがC2\_\_G26に供給され、コンテンツキーが導出される。コンテンツキーがC2\_\_ECBC27に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ13がDVDメディア1に記録される。

## 【0033】

プレーヤ3においては、CCIとタイトルキーとがC2\_\_G36に供給され、コンテンツキーが導出される。コンテンツキーがC2\_\_ECBC37に供給され、DVDメディア1から再生された暗号化コンテンツ13がコンテンツキーを鍵として復号される。

## 【0034】

図1の構成において、レコーダ2による記録の手順について説明する。レコーダ2は、DVDメディア1からMKB12を読み出し、プロセスMKB22によってデバイスキー21とMKB12とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー21（レコーダ2の機器またはアプリケーション）がMKBによってリボークされたと判定され、レコーダ2は、以後の処理を中断し、DVDメディア1への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

## 【0035】

次に、レコーダ2は、DVDメディア1からメディアID11を読み、メディアキーと共にメディアIDをC2\_\_G23に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器24で発生させたタイトルキーがC2\_\_E25で暗号化され、暗号化タイトルキー14としてDVDメディア1に記録される。また、タイトルキーとコンテンツのCCI情報がC2\_\_G26で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをC2\_\_ECBC

27で暗号化し、DVDメディア1上に暗号化コンテンツ13としてCCI15と共に記録する。

#### 【0036】

プレーヤ3による再生の手順について説明する。最初にMKB12をDVDメディア1から読み出し、デバイスキー31とMKB12を演算し、リボケーションの確認がなされる。デバイスキー31、すなわち、プレーヤ3の機器またはアプリケーションがリボークされない場合には、メディアIDを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー14とメディアユニークキーからタイトルキーが演算される。タイトルキーとCCI15とがC2\_\_G36に入力され、コンテンツキーが導出される。コンテンツキーがC2\_\_DCBC37に入力され、コンテンツキーを鍵として、DVDメディア1から再生された暗号化コンテンツ13に対してC2\_\_DCBC37の演算が施される。その結果、暗号化コンテンツ13が復号される。

#### 【0037】

このように、コンテンツの復号に必要なコンテンツキーを得るためには、DVDメディアの1枚毎に異なるメディアIDが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアIDがオリジナルのメディアIDと異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

#### 【0038】

上述した図1の構成は、記録再生機器として構成されたものである。この発明は、DVDメディア1に対するコンテンツ保護処理をPC環境下で扱う場合に適用される。図2を参照して現行の方式によるPCとドライブの役割分担を示す。図2において、参照符号4が上述したCPRM規格に準拠したDVDメディア1を記録および再生する記録再生装置としてのDVDドライブを示す。

#### 【0039】

参照符号5がデータ処理装置としてのホスト例えばPCを示す。ホスト5は、DVDメディア1に記録可能で、DVDメディア1から再生可能なコンテンツを扱うことができ、且つDVDドライブ4と接続されてデータ交換が可能な装置ま

たはアプリケーションソフトウェアである。例えばPCに対してアプリケーションソフトウェアがインストールされることによってホスト5が構成される。

#### 【0040】

DVDドライブ4とホスト5との間がインターフェース4aで接続されている。インターフェース4aは、ATAPI(AT Attachment with Packet Interface), SCSI(Small Computer System Interface), USB(Universal Serial Bus), IEEE(Institute of Electrical and Electronics Engineers)1394等である。

#### 【0041】

DVDメディア1には、メディアID11、メディアキープブロック12およびACC(Authentication Control Code)が予め記録されている。ACCは、DVDドライブ4とホスト5との間の認証がDVDメディア1によって異なるようにするために予めDVDメディア1に記録されたデータである。

#### 【0042】

DVDドライブ4は、ACC16をDVDメディア1から読み出す。DVDメディア1から読み出されたACC16がDVDドライブ4のAKE(Authentication and Key Exchange)41に入力されると共に、ホスト5へ転送される。ホスト5は、受け取ったACCをAKE51に入力する。AKE41および51は、乱数データを交換し、この交換した乱数とACCの値とから認証動作の度に異なる値となる共通のセッションキー(図2の構成においてはバスキーと称する)を生成する。

#### 【0043】

バスキーがMAC(Message Authentication Code)演算ブロック42および52にそれぞれ供給される。MAC演算ブロック42および52は、AKE41および51でそれぞれ得られたバスキーをパラメータとして、メディアIDおよびメディアキープブロック12のMACを計算するプロセスである。MKBとメディアIDの完全性(integrity)をホスト5が確認するために利用される。

#### 【0044】

MAC42および52によってそれぞれ計算されたMACがホスト5の比較5

3において比較され、両者の値が一致するかどうか判定される。これらのMACの値が一致すれば、MKBとメディアIDの完全性が確認されたことになる。比較出力でスイッチSW1が制御される。

#### 【0045】

スイッチSW1は、DVDドライブ4のDVDメディア1の記録または再生経路と、ホスト5の暗号化／（または）復号モジュール54との間の信号路をON／OFFするものとして示されている。なお、スイッチSW1は、信号路のON／OFFを行うものとして示されているが、より実際には、ONの場合にホスト5の処理が継続し、OFFの場合にホスト5の処理が停止することを表している。暗号化／復号モジュール54は、メディアユニークキーと暗号化タイトルキーとCCIとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ13へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ13を復号する演算ブロックである。

#### 【0046】

メディアユニークキー演算ブロック55は、MKB12とメディアIDとデバイスキー56とからメディアユニークキーを演算する演算ブロックである。すなわち、図1に示すレコーダまたはプレーヤと同様に、デバイスキーとMKB12とからメディアキーが演算され、さらに、メディアキーとメディアID11とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック55は、リボケーションを行うリボーク処理部としての機能も有する。

#### 【0047】

記録時に、比較53によって完全性が確認された場合には、スイッチSW1がONされ、暗号化／復号モジュール54からスイッチSW1を通じてドライブ4に対して、暗号化コンテンツ13、暗号化タイトルキー14およびCCI15が供給され、DVDメディア1に対してそれぞれ記録される。再生時に、比較53によって完全性が確認された場合には、スイッチSW1がONされ、DVDメディア1からそれぞれ再生された暗号化コンテンツ13、暗号化タイトルキー14

およびCCI15がスイッチSW1を通じてホスト5の暗号化／復号モジュール54に対して供給され、暗号化コンテンツが復号される。

#### 【0048】

図3は、図2に示す現行のPC環境下のDVDメディアを利用するシステムにおいて、DVDメディア1と、DVDドライブ4と、ホスト5との間の信号の授受の手順を示す。ホスト5がDVDドライブ4に対してコマンドを送り、DVDドライブ4がコマンドに応答した動作を行う。

#### 【0049】

最初に、ホスト5からの要求に応じてDVDメディア1上のACCがシークされ、読み出される（ステップS1）。次のステップS2において、読み出されたACCがAKE41に入力されると共に、ホスト5へ転送され、ホスト5では、受け取ったACCがAKE51へ入力される。AKE41および51は、乱数データを交換し、この交換した乱数とACC16の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをDVDドライブ4とホスト5が共有する。相互認証が成立しなかった場合では、処理が中断する。

#### 【0050】

認証動作は、電源のON後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

#### 【0051】

認証が成功すると、次に、ステップS3において、ホスト5がDVDドライブ4に対して、DVDメディア1からのMKB（メディアキープロック）パック#0の読み出しを要求する。MKBは、パック0～パック15の16セクタが12回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

#### 【0052】

DVDドライブ4がステップS4においてMKBのパック#0を読みに行き、ステップS5において、パック#0が読み出される。DVDドライブ4は、モデ

ィフアイドMKBをホスト5へ戻す(ステップS6)。すなわち、MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を付加してホスト5へデータを転送する。パック#0以外の残りのMKBパックの要求と、DVDドライブ4の読み出し動作と、モディフアイドMKBパックの転送動作とがMKBのパックがなくなるまで、例えばパック#15が読み出され、ホスト5へ転送されるまで、ステップS7およびS8によって繰り返される。

#### 【0053】

次に、ホスト5がDVDドライブ4に対してメディアIDを要求する。DVDドライブ4がDVDメディア1に記録されているメディアIDを読みに行き、ステップS11において、メディアIDが読み出される。DVDドライブ4は、メディアIDを読み出す際に、バスキーをパラメータとしてそのMAC値を計算し、ステップS12において、読み出されたメディアIDに対してMAC値m1を付加してホスト5へデータを転送する。

#### 【0054】

ホスト5では、DVDドライブ4から受け取ったMKB12およびメディアID11からバスキーをパラメータとして再度MAC値を計算し、計算したMAC値とDVDドライブ4から受け取ったMAC値とを比較53で比較し、両者が一致したならば、正しいMKBおよびメディアIDを受け取ったと判定して、スイッチSW1をONに設定して処理を先に進める。逆に両者が一致しなかったならば、MKBおよびメディアIDが改ざんされたものと判定して、スイッチSW1をOFFに設定して処理を中断する。

#### 【0055】

ステップS13において、ホスト5がDVDドライブ4に対して暗号化コンテンツを要求し、ステップS14において、DVDドライブ4が暗号化コンテンツを読み出し、ステップS13において、読み出した暗号化コンテンツがホスト5に転送される。ホスト5のメディアユニークキー演算ブロック55では、デバイスキー56とMKB12とメディアID11とによってメディアユニークキーが計算される。そして、メディアユニークキーが暗号化/復号モジュール54に供



給され、暗号化タイトルキー14、CCI15からコンテンツキーが求められ、コンテンツキーを鍵としてDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

#### 【0056】

図4のフローチャートにおいて、ステップST1は、MAC演算ブロック42でバスキーをパラメータとして求められたMAC計算値と、MAC演算ブロック53でバスキーをパラメータとして求められたMAC計算値とを比較するステップである。両者が一致すれば、スイッチSW1がステップST2においてONとされ、両者が一致しない場合では、スイッチSW1がステップST3においてOFFとされ、処理が停止する。

#### 【0057】

上述したCPRMでは、DVD-Videoの著作権保護技術であるCSSと同じバスキー生成方法を採用している。CSS認証方式の内容は、本来秘密であるべき情報であるが、既に解析され一般ユーザーが入手可能なCSSライセンス管理団体であるDVD-CCAの許諾を得ていないフリーソフトウェアによって動作させることが可能となっている。また、コンテンツプロテクション処理は、ホスト側でなされる、すなわち、リボケーション判定、メディアキー取得、メディアユニークキー導出、タイトルキー生成・導出からコンテンツキー導出およびコンテンツ暗号化・復号の全てがホスト側の処理であることから、著作権保護技術としての信頼性が低下している。

#### 【0058】

以下に述べるこの発明の一実施形態では、かかる問題点を解決するものである。一実施形態では、PC環境下でのコンテンツプロテクション処理におけるタイトルキー導出に関わる構成をドライブ内部に持ち、PCとの相互認証を経てタイトルキーおよびコンテンツキーをPCに送信するものである。

#### 【0059】

図5は、一実施形態における相互認証の構成を示すブロック図であり、図6は、ドライブ側の処理の流れを示すフローチャートであり、図7は、ホスト側の処

理の流れを示すフローチャートである。以下の説明において、参照符号101がメディア例えば光ディスクを示し、参照符号102がメディアのドライブを示し、参照符号103がドライブ102とドライバーストインターフェース104を介して接続されたホストを示す。メディア101は、上述したDVDメディアと同様の情報が予め記録されているものである。メディア101は、記録可能なものに限り、読み出し専用のもので良い。ホスト103がドライブ102に対して所定のコマンドを送り、その動作を制御する。使用するコマンドは、上述した非特許文献2に記載されているコマンド並びにコマンドを拡張したもの、および、メディア101からコンテンツをセクタ・データとして読み出すためのREADコマンド、メディア101へコンテンツをセクタ・データとして書き込むためのWRITEコマンドである。

#### 【0060】

ドライブ102は、ドライブのデバイスキー121を有し、ホスト103がホストのデバイスキー131を有している。デバイスキー121は、多くの場合にLSI (Large Scale Integrated Circuit: 大規模集積回路) 内部に配置され、外部から読み出すことができないようセキュアに記憶される。デバイスキー131は、ソフトウェアプログラム内にセキュアに記憶される場合と、ハードウェアとしてセキュアに記憶される場合とがある。また、ドライブ102がメディア101を扱う正当なドライブとなるためには、一実施形態のように、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

#### 【0061】

図5に示すように、ドライブ102には、MKBとデバイスキー121とが入力され、ドライブのデバイスキーがリボケーションされたかどうかを判定するプロセスMKB122が備えられている。ホスト103にも同様に、プロセスMKB132が備えられている。リボケーションされない場合に、プロセスMKB122および132からそれぞれメディアキーKmが出力される。リボーク判定処理がなされ、メディアキーKmが得られてから認証処理がなされる。

## 【0062】

参照符号123、124および125は、メディアキーKmをパラメータとしてMAC値を計算するMAC演算ブロックをそれぞれ示す。また、参照符号126、127および128は、乱数発生器(RNG: Random Number Generator)をそれぞれ示す。乱数発生器126が乱数Ra1を生成し、乱数発生器127が乱数Ra2を生成し、乱数発生器128が乱数Ra3を生成する。乱数発生器126、127、128は、例えばLSIの構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウェアとしても良いが、乱数Ra1、Ra2、Ra3は、互いに独立したものである。

## 【0063】

ホスト103に、メディアキーKmをパラメータとしてMAC値を計算するMAC演算ブロック133、134および135と、乱数発生器136、137および138が備えられている。乱数発生器136が乱数Rb1を生成し、乱数発生器137が乱数Rb2を生成し、乱数発生器138が乱数Rb3を生成する。乱数発生器136、137、138は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

## 【0064】

ドライブ102において生成された乱数とホスト103において生成された乱数とが交換される。すなわち、乱数Ra1および乱数Rb1がMAC演算ブロック123および133に入力され、乱数Ra2および乱数Rb2がMAC演算ブロック124および134に入力され、乱数Ra3および乱数Rb3がMAC演算ブロック125および135に入力される。

## 【0065】

ドライブ102のMAC演算ブロック123が演算したMAC値と、ホスト103のMAC演算ブロック133が演算したMAC値とがホスト103内の比較139において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、 $eKm(Ra1 \parallel Rb1)$ と表記される。 $eKm()$ は、メディアキーKmを鍵とし

て括弧内のデータを暗号化することを表している。Ra1 || Rb1の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、ホスト103によるドライブ102の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

#### 【0066】

ホスト103のMAC演算ブロック134が演算したMAC値と、ドライブ102のMAC演算ブロック124が演算したMAC値とがドライブ102内の比較129において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、eKm(Rb2 || Ra2)と表記される。比較の結果、二つの値が同一と判定されると、ドライブ102によるホスト103の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

#### 【0067】

かかる相互認証において、比較139および129の両者において、MAC値が同一と判定され、ドライブ102およびホスト103の両者の正当性が確認されると、すなわち、相互認証が成功すると、MAC演算ブロック125および135によって、共通のセッションキーeKm(Ra3 || Rb3)がそれぞれ生成される。

#### 【0068】

さらに、上述した相互認証の処理の流れを図6および図7のフローチャートを参照して説明する。最初に、図7のステップST20において、ホスト103がドライブ102に対して、コマンドREPORT KEYを発行し、MKBの転送を要求する。図6のステップST10において、ドライブ102がメディア101からMKB112を読み出して、ホスト103へ転送する。

#### 【0069】

次に、ドライブ102がステップST11において、プロセスMKB122によってメディアキーKmを計算し、ホスト103がステップST21において、プロセスMKB132によってメディアキーKmを計算する。この計算の過程でそれぞれが内蔵するデバイスキー121および131がリボケーションの対象とされているか否かが自分自身によって確認される（図6中のステップST12、

図7中のステップST22)。

#### 【0070】

ドライブ102およびホスト103のそれぞれは、リボケーションの対象とされている場合にはリボークされ、処理が終了する。若し、ホスト103がリボケーションの対象とされていないければ、ステップST23において、コマンドSEND KEYにより、ドライブ102に対して乱数発生器136および137でそれぞれ生成された乱数Rb1と乱数Rb2を転送する。若し、ドライブ102がリボケーションの対象とされていないければ、ステップST13において、ドライブ102がホスト103から転送されたこれらの乱数を受け取る。

#### 【0071】

その後、ホスト103は、コマンドREPORT KEYによりドライブ102に対してドライブ102が持つメディアキーKmを鍵としたMACによるレスポンス値と乱数生成器126が発生した乱数Ra1とをホスト103へ転送することを要求する(ステップST24)。このレスポンス値は、 $eKm(Ra1 \parallel Rb1)$ と表記される。 $eKm()$ は、メディアキーKmを暗号鍵として括弧内のデータを暗号化することを表している。 $Ra1 \parallel Rb1$ の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。

#### 【0072】

ホスト103からコマンドREPORT KEYを受け取ったドライブ102は、ステップST14において、MAC演算ブロック123が生成したMAC値 $eKm(Ra1 \parallel Rb1)$ と乱数Ra1をホスト103へ転送する。ステップST25において、ホスト103は、自身のMAC演算ブロック133でMAC値を計算し、比較139においてドライブ102から受け取った値と一致するかの確認を行う。若し、受け取ったMAC値と計算されたMAC値とが一致したのなら、ホスト103によるドライブ102の認証が成功したことになる。ステップST25における比較の結果が同一でない場合には、ホスト103によるドライブ102の認証が失敗したことになる、リジェクト処理がなされる。

#### 【0073】

ホスト103によるドライブ102の認証が成功した場合には、ステップST

26において、ホスト103がドライブ102へコマンドREPORT KEYを送付し、ドライブ102の乱数生成器124および125がそれぞれ生成する乱数Ra2と乱数Ra3の転送を要求する。このコマンドに応答して、ステップST15において、ドライブ102は、これらの乱数をホスト103へ転送する。

#### 【0074】

ステップST27において、ホスト103のMAC演算ブロック134は、ドライブ102から受け取った乱数からホスト103が持つメディアキーKmを鍵としたMACによるレスポンス値eKm(Rb2 || Ra2)を計算し、乱数Rb3とともに、コマンドSEND KEYを用いてドライブ102へ転送する。

#### 【0075】

ステップST16において、ドライブ102は、ホスト103からレスポンス値eKm(Rb2 || Ra2)および乱数Rb3を受け取ると、自身でMAC値を計算し、ステップST17において、比較129によってホスト103から受け取ったMAC値と一致するかの確認を行う。若し、受け取ったMAC値と計算されたMAC値とが一致したのなら、ドライブ102によるホスト103の認証が成功したことになる。この場合には、ステップST18において、MAC演算ブロック125がセッションキーeKm(Ra3 || Rb3)を生成し、また、ホスト103に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッションキーは、認証動作の度に異なる値となる。

#### 【0076】

ステップST17における比較の結果が同一でない場合には、ドライブ102によるホスト103の認証が失敗したことになり、ステップST19において、認証が失敗したことを示すエラー情報がホスト103に送信される。

#### 【0077】

ホスト103は、送付したコマンドSEND KEYに対する応答としてドライブ102から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップST28において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステ

ップST29において、MAC演算ブロック135がドライブ側と共通のセッションキー $eKm(Ra3 \parallel Rb3)$  (例えば64ビット長) を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。セッションキー $eKm(Ra3 \parallel Rb3)$ を以下の説明では、適宜 $Ks$ と表記する。

#### 【0078】

上述した一実施形態による相互認証は、ドライブ102がリボケーション機能を持つことができ、また、認証専用の特定の認証鍵を必要としない特徴を有している。

#### 【0079】

さらに、ドライブ102が比較129によってホスト103の認証結果を確認することで、ドライブ102がホスト103から正規のライセンスを受けた上で実装されたものであるか否かを判定することが可能となる。

#### 【0080】

次に、上述した相互認証を行うドライブ102とホスト103とを組み合わせで実現したレコーダの一実施形態の構成を図8に示す。一実施形態のレコーダは、ドライブ102が計算したメディアユニークキーを相互認証によって生成したセッションキー $Ks$ を用いてセキュアにホスト103に転送する。また、ドライブ102の乱数発生器143によってタイトルキーが生成される。ドライブ102においてタイトルキーおよびCCIからコンテンツキーが生成され、生成されたコンテンツキーがセッションキー $Ks$ を用いてホスト103へセキュアに転送され、ホスト103が復号したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ102へ転送し、ドライブ102が暗号化コンテンツ、暗号化タイトルキーおよびCCIをメディア101へ記録する構成とされている。すなわち、ドライブ102において、メディアユニークキーおよびコンテンツキーを生成している。

#### 【0081】

レコーダを構成するドライブ102は、デバイスキー121、プロセスMKB122、C2\_\_G2141、DES(Data Encryption Standard)エンクリプタ142、乱数発生器143、C2\_\_G145、DESエンクリプタ146の構成要

素を有する。C2\_\_G2141は、メディアIDとメディアキーからメディアユニークキーを演算するブロックである。C2\_\_G2145は、タイトルキーとCCIとからコンテンツキーを演算するブロックである。

#### 【0082】

メディア101から再生されたMKB112とデバイスキー121とがプロセスMKB122において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスMKB122において、MKB112とデバイスキー121からメディアキーが算出される。MKB112の中にドライブ102のデバイスキー121が入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキー121を持つドライブ102が正当なものでないと判断され、ドライブ102がリボケーションされる。

#### 【0083】

C2\_\_G141は、メディアキーとメディアID111とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがDESエンクリプタ142にてセッションキーKsによって暗号化される。暗号化の方式として、例えばDES CBCモードが使用される。DESエンクリプタ142の出力がホスト103のDESデクリプタ151に送信される。

#### 【0084】

ドライブ102の乱数発生器143によってタイトルキーが生成され、乱数発生器143からのタイトルキーがホスト103のC2\_\_E153に供給され、タイトルキーがメディアユニークキーを使用してC2によって暗号化される。暗号化タイトルキー114がメディア101に記録される。

#### 【0085】

ホスト103において、セッションキーKsを鍵としてMAC演算ブロック158によりCCIのMAC値eKs(CCI)が計算され、CCIとともにドライブ102へ転送される。

#### 【0086】

ドライブ102において、ホスト103から受け取ったCCIからセッションキーKsを鍵としてMAC演算ブロック157によりCCIのMAC値eKs(



CCI) が計算され、ホスト 103 から受け取った MAC 値とともに比較 159 へ供給される。

#### 【0087】

比較 159 では、両方の MAC 値が一致したならば、ホスト 103 から受け取った CCI の改ざんは無いものと判断し、スイッチ SW2 を ON する。一致しなかった場合は、CCI は改ざんされたものとみなし、スイッチ SW2 を OFF し、以降の処理を中断する。

#### 【0088】

ドライブ 102 において、ホスト 103 から受け取った CCI とタイトルキーとが C2\_\_G145 に供給され、コンテンツキーが導出される。コンテンツキーが DES エンクリプタ 146 に供給され、セッションキー Ks を鍵として、コンテンツキーが暗号化される。暗号化コンテンツキーがホスト 103 の DES デクリプタ 156 に転送される。

#### 【0089】

ホスト 103 の DES デクリプタ 156 でセッションキー Ks を鍵として復号されたコンテンツキーが C2\_\_ECBC155 に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ 113 がドライブ 102 に転送され、ドライブ 102 によってメディア 101 に記録される。

#### 【0090】

図 9 は、レコーダの一実施形態によるコンテンツ記録時の手順を示すものである。最初に、ホスト 103 からの要求に応じてメディア 101 上の MKB がシークされ、読み出される (ステップ S61)。次のステップ S62 の AKE (Authentication and Key Exchange) において、上述したようなりボーク処理とドライブ 102 とホスト 103 の相互認証動作がなされる。

#### 【0091】

相互認証動作は、電源の ON 後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

## 【0092】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ102およびホスト103の両者において、セッションキー $K_s$ が生成され、セッションキー $K_s$ が共有される。

## 【0093】

次のステップS63において、ホスト103がドライブ102に対してメディアユニークキーを要求する。ドライブ102は、メディア101のメディアIDをシークし（ステップS64）、メディアIDをメディア101から読み出す（ステップS65）。ドライブ102は、メディアキーとメディアIDとを演算することによってメディアユニークキーを生成する。ステップS66において、メディアユニークキーがセッションキー $K_s$ によって暗号化され、暗号化されたメディアユニークキーがホスト103に転送される。

## 【0094】

次に、ステップS67において、ホスト103がドライブ102に対してタイトルキーを要求する。ステップS68において、ドライブ102がタイトルキーをホスト103に転送する。ホスト103において、セッションキー $K_s$ によって、暗号化されたメディアユニークキーが復号される。そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。

## 【0095】

また、ステップS69において、ホスト103がドライブ102に対してCCIを送る。このとき、CCIの改ざんを回避するためにCCIの認証データとして計算されたMAC値 $e K_s$  (CCI)を付加して転送する。ドライブ102において、CCIの改ざんが無いことを確認後、タイトルキーとCCIからコンテンツキーが生成され、コンテンツキーがセッションキー $K_s$ で暗号化される。ステップS70において、ホスト103がドライブ102に対してコンテンツキーを要求すると、ステップS71において、ドライブ102が暗号化されたコンテンツキーをホスト103に送る。

## 【0096】

ホスト103は、暗号化コンテンツキーをセッションキー $K_s$ によって復号し

、コンテンツキーを得る。コンテンツキーによってコンテンツが暗号化される。ステップS72において、ホスト103からドライブ102に対して、暗号化タイトルキー、暗号化コンテンツおよびCCIが転送される。ステップS73において、ドライブ102によって、暗号化タイトルキー、暗号化コンテンツおよびCCIがメディア101に対して記録される。

#### 【0097】

上述した図8に示す構成のレコーダは、ドライブ102において、真正乱数またはそれに近い乱数をハードウェア例えばLSIによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。また、ドライブ102において、ハードウェア構成によってコンテンツキーを生成するので、著作権保護の実装を強力とすることができる。

#### 【0098】

次に、上述した相互認証を行うドライブ102とホスト103とを組み合わせで実現したプレーヤの一実施形態の構成を図10に示す。一実施形態のプレーヤは、ドライブ102が計算したメディアユニークキーを相互認証によって生成したセッションキーKsを用いてセキュアにホスト103に転送し、ホスト103が暗号化タイトルキーをメディアユニークキーによって復号し、タイトルキーとCCIとから導出したコンテンツキーを用いてコンテンツを復号する構成とされている。

#### 【0099】

プレーヤを構成するドライブ102は、デバイスキー121、プロセスMKB122、C2\_\_G2141、DESエンクリプタ142の構成要素を有する。メディア101から再生されたMKB112とデバイスキー121とがプロセスMKB122において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスMKB122において、MKB112とデバイスキー121からメディアキーが算出される。

#### 【0100】

C2\_\_G141は、メディアキーとメディアID111とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがDESエンクリプ

タ 1 4 2 にてセッションキー  $K_s$  によって暗号化される。暗号化の方式として、例えば DES CBC モードが使用される。DES エンクリプタ 1 4 2 の出力がホスト 1 0 3 の DES デクリプタ 1 5 1 に送信される。

#### 【0101】

ホスト 1 0 3 において、DES デクリプタ 1 5 1 において、セッションキー  $K_s$  によってメディアユニークキーが復号される。メディアユニークキーおよび暗号化タイトルキー 1 1 4 が C 2 \_ D 1 5 3 に供給され、暗号化タイトルキーがメディアユニークキーを使用して復号される。復号されたタイトルキーとメディア 1 0 1 から再生された C C I が C 2 \_ G 1 5 4 に供給され、コンテンツキーが導出される。メディア 1 0 1 から再生された暗号化コンテンツ 1 1 3 が C 2 デクリプタ 1 5 5 において、コンテンツキーによって復号され、コンテンツキーが得られる。

#### 【0102】

図 1 1 は、コンテンツ再生時の手順を示すものである。最初に、ホスト 1 0 3 からの要求に応じてメディア 1 0 1 上の MKB がシークされ、読み出される（ステップ S 4 1）。MKB がパック毎に読み出される。次のステップ S 4 2 の A K E において、上述したようなりボーク処理と、ドライブ 1 0 2 とホスト 1 0 3 の相互認証動作がなされる。

#### 【0103】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ 1 0 2 およびホスト 1 0 3 の両者において、セッションキー  $K_s$  が生成され、セッションキー  $K_s$  が共有される。

#### 【0104】

次のステップ S 4 3 において、ホスト 1 0 3 がドライブ 1 0 2 に対してメディアユニークキーを要求する。ドライブ 1 0 2 は、メディア 1 0 1 のメディア ID をシークし（ステップ S 4 4）、メディア ID をメディア 1 0 1 から読み出す（ステップ S 4 5）。ドライブ 1 0 2 は、メディアキーとメディア ID とを演算することによってメディアユニークキーを生成する。ステップ S 4 6 において、メディアユニークキーがセッションキー  $K_s$  によって暗号化され、暗号化されたメ

ディアユニークキーがホスト103に転送される。

#### 【0105】

次に、ステップS47において、ホスト103がドライブ102に対して、暗号化タイトルキー、CCIおよび暗号化コンテンツを要求する。ステップS48において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113をメディア101からリードする。ステップS49において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113を読み取る。そして、ステップS50において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113をホスト103に対して転送する。

#### 【0106】

ホスト103において、タイトルキーが復号され、タイトルキーとCCIとからコンテンツキーが求められ、コンテンツキーを鍵として暗号化コンテンツが復号される。

#### 【0107】

図10に示すプレーヤの構成においては、ホスト103が暗号化タイトルキーを復号するデクリプタC2\_\_D153を備えているが、ドライブ102が暗号化タイトルキーを復号するデクリプタを備えるようにしても良い。この場合、復号されたタイトルキーがホスト103のコンテンツキー生成用のC2\_\_G154に対してセキュアに転送される。または、ドライブ102にコンテンツキー生成装置C2\_\_Gを設け、ドライブ102において復号されたタイトルキーとCCIとからコンテンツキーを生成するようにしても良い。この場合、復号されたコンテンツキーがホスト103のC2\_\_DCBC155へセキュアに転送される。

#### 【0108】

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばタイトルキーは、タイトル毎のキーであるが、この発明では、乱数情報であれば、タイトル毎に異なることは、必要ではない。

#### 【0109】

また、上述した説明においては、著作権保護技術としてCPRMおよびCPRMを拡張した例を挙げたが、CPRM以外の著作権保護技術に対してもこの発明を適用することができる。例えば、特開2001-352322号公報において提案されるツリー構造の鍵配布構成に基づく著作権保護技術に対して適用可能である。また、PCベースのシステムに対してこの発明が適用されるが、このことは、PCとドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

#### 【0110】

##### 【発明の効果】

この発明では、再生装置側でコンテンツキーを生成し、コンテンツキーを情報処理装置へ送信し、情報処理装置側でコンテンツキーによってコンテンツを暗号化している。このように著作権保護のための鍵情報の生成を再生装置で行うので、ハードウェア構成でコンテンツキーを生成することが可能となり、耐タンパー性を高めることができる。また、再生装置において、乱数を生成し、乱数を中間鍵とするので、再生装置において、真正乱数またはそれに近い乱数をハードウェア例えばLSIによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。このように、この発明では、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持たせることが容易に実施でき、また、ディスクからのデータとしてそのまま読み出された暗号化コンテンツが「DeCSS」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を防ぐことができることから、著作権保護技術の安全性を確保することができる。

#### 【0111】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことに

よって、記録再生装置自身をリボークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばLSIによって生成できるので、PC内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

#### 【図面の簡単な説明】

##### 【図1】

先に提案されているレコーダ、プレーヤおよびDVDメディアからなるシステムを説明するためのブロック図である。

##### 【図2】

PCベースのDVDメディア記録再生システムを説明するためのブロック図である。

##### 【図3】

図2のシステムにおけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

##### 【図4】

図2のシステムにおける認証動作を説明するためのフローチャートである。

##### 【図5】

この発明の一実施形態による相互認証のための構成を示すブロック図である。

##### 【図6】

この発明の一実施形態におけるドライブの認証動作の処理の手順を説明するためのフローチャートである。

##### 【図7】

この発明の一実施形態におけるホストの認証動作の処理の手順を説明するためのフローチャートである。

##### 【図8】

この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の一例をブロック図である。

## 【図 9】

レコーダの一例の通信の手順を説明するための略線図である。

## 【図 10】

この発明の一実施形態によるドライブとホストを組み合わせたプレーヤの構成の一例をブロック図である。

## 【図 11】

プレーヤの一例の通信の手順を説明するための略線図である。

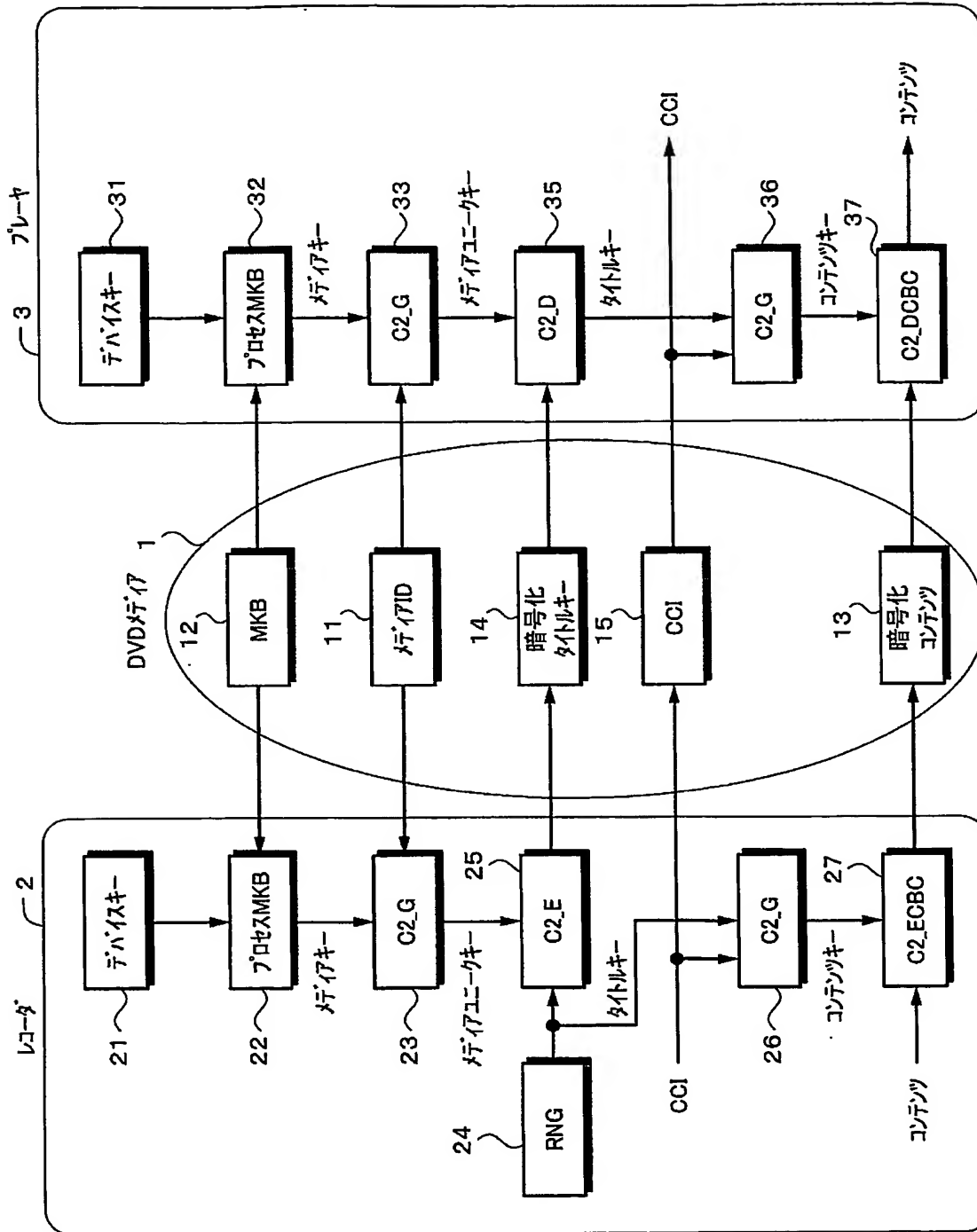
## 【符号の説明】

1・・・DVDメディア、2・・・レコーダ、3・・・プレーヤ、4・・・DVDドライブ、4a・・・インターフェース、5・・・ホスト、11・・・メディアID、12・・・メディアキーブロック(MKB)、13・・・暗号化コンテンツ、42, 52・・・MAC演算ブロック、46・・・デバイスキー、46a・・・デバイスキーの前半部、47・・・DESエンクリプタ、48・・・メディアユニークキー演算ブロック、49, 49a・・・DESエンクリプタ、49b・・・DESデクリプタ、53・・・MACを比較する比較、54・・・暗号化/復号モジュール、55・・・メディアユニークキー演算ブロック、101・・・メディア、102・・・ドライブ、103・・・ホスト、104・・・インターフェース、121・・・ドライブのデバイスキー、122・・・プロセスMKB、123, 124, 125・・・ドライブのMAC演算ブロック、126, 127, 128・・・ドライブの乱数発生器、129・・・比較、131・・・ホストのデバイスキー、132・・・プロセスMKB、133, 134, 135・・・ホストのMAC演算ブロック、136, 137, 138・・・ホストの乱数発生器、139・・・比較、141, 154・・・C2\_\_G、142・・・DESエンクリプタ、143・・・乱数発生器、151, 156・・・DESデクリプタ、153・・・C2\_\_E、155・・・C2\_\_EBC、157, 158・・・MAC演算ブロック、159・・・比較

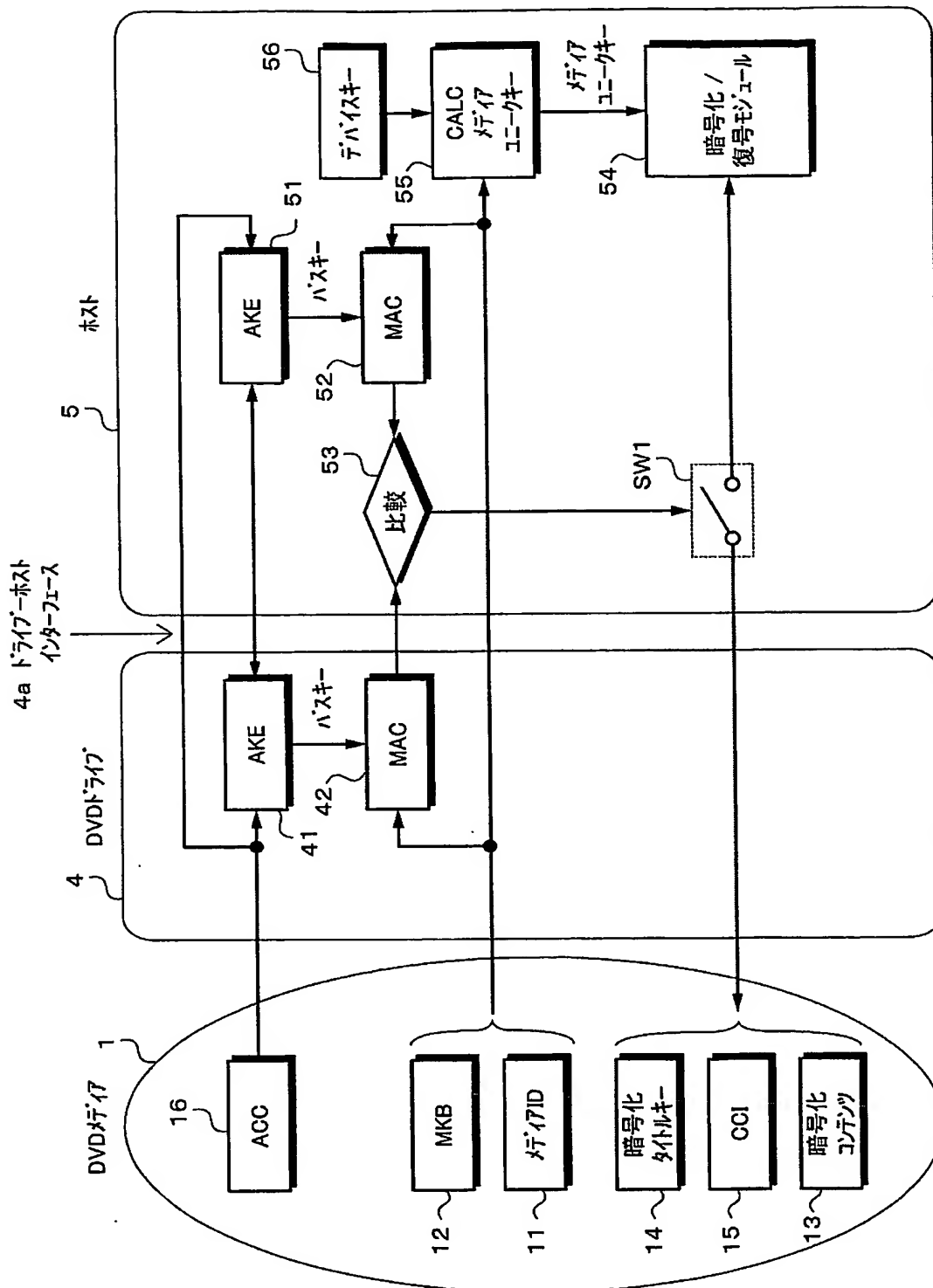


【書類名】 図面

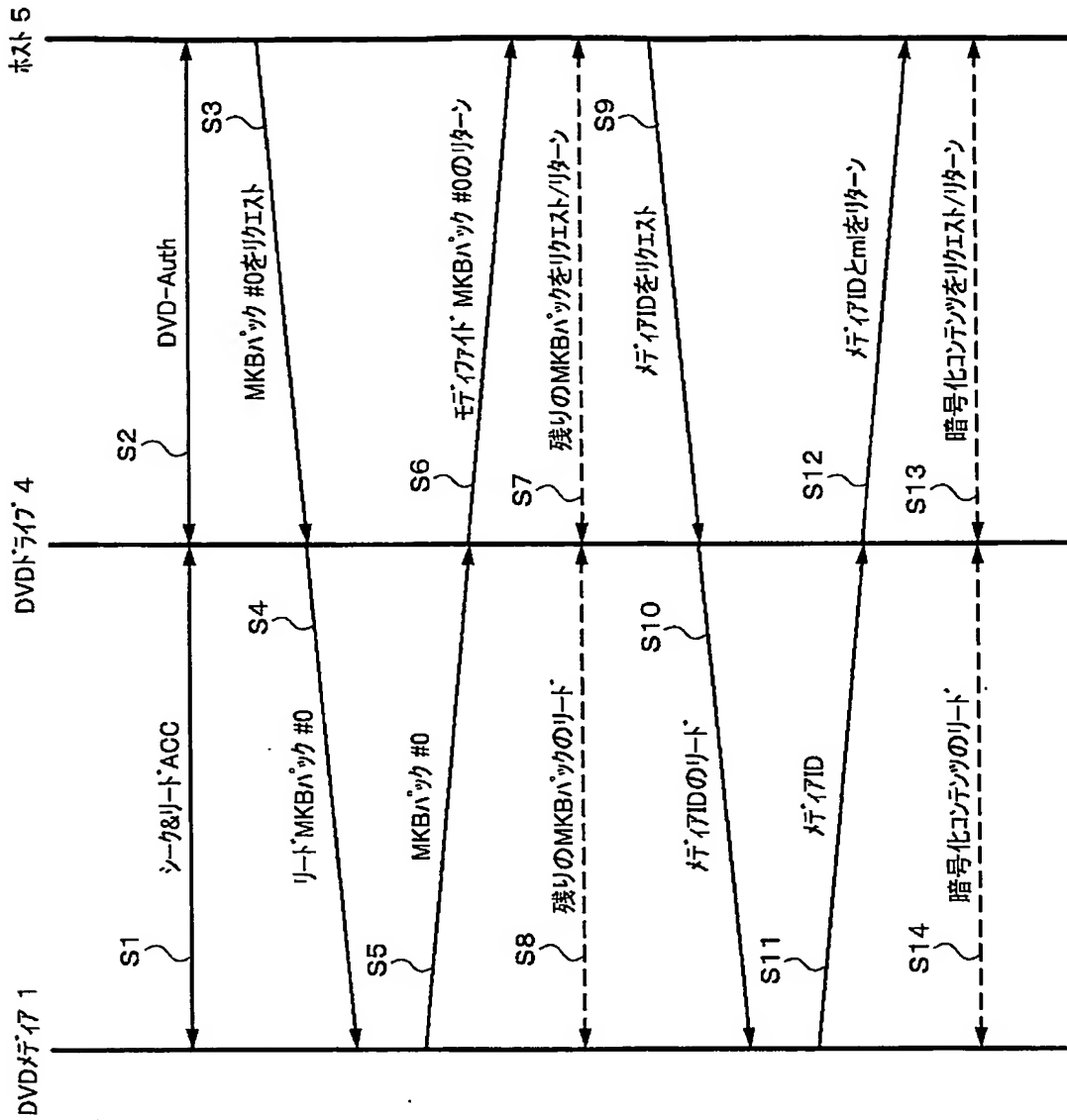
【図 1】



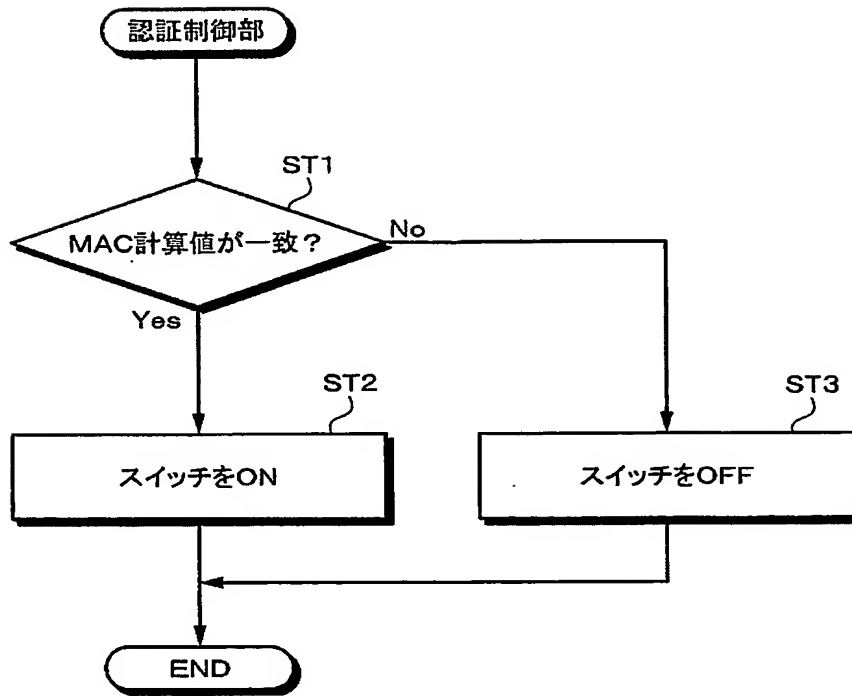
【図 2】



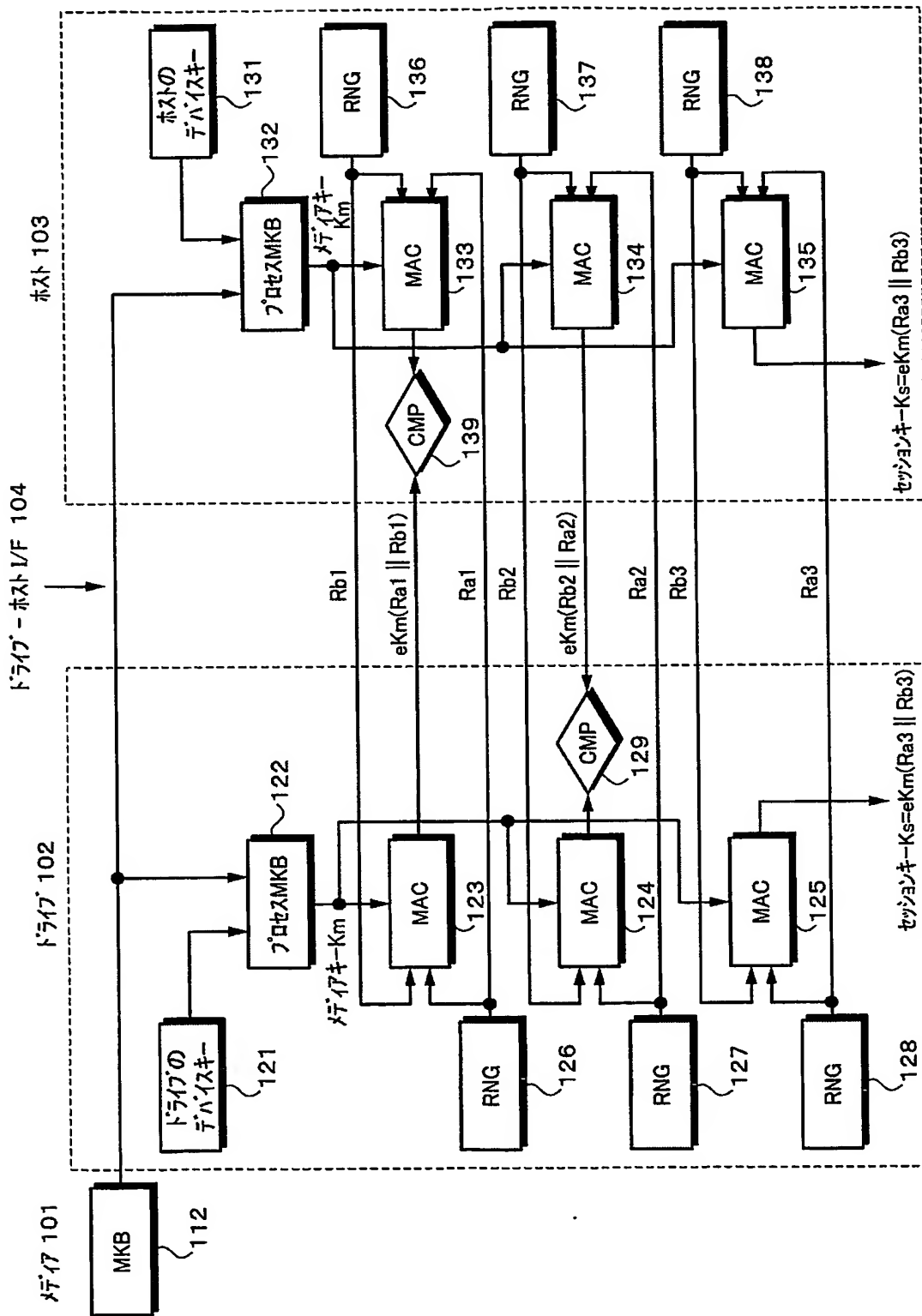
【図 3】



【図 4】

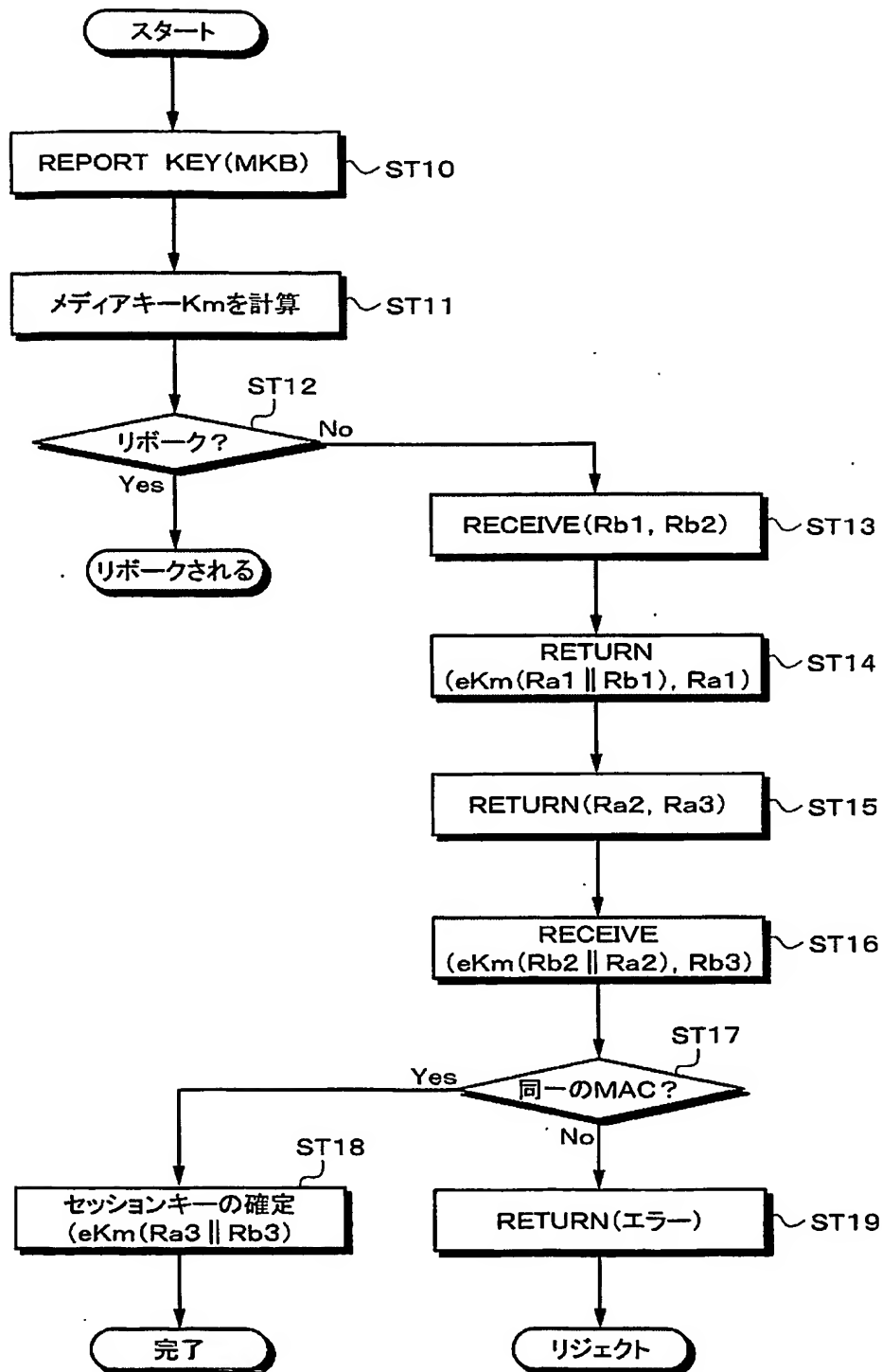


【図 5】

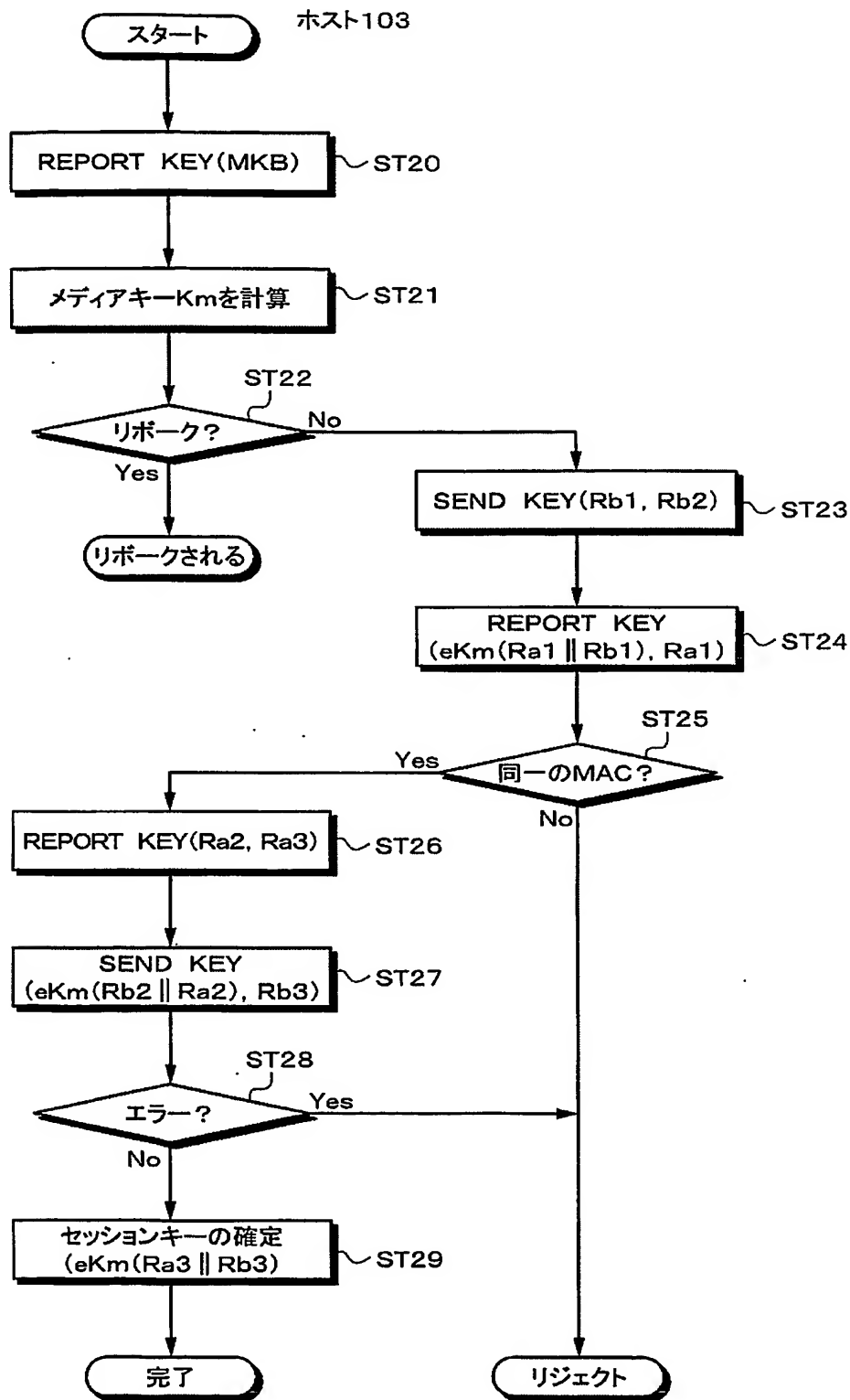


【図 6】

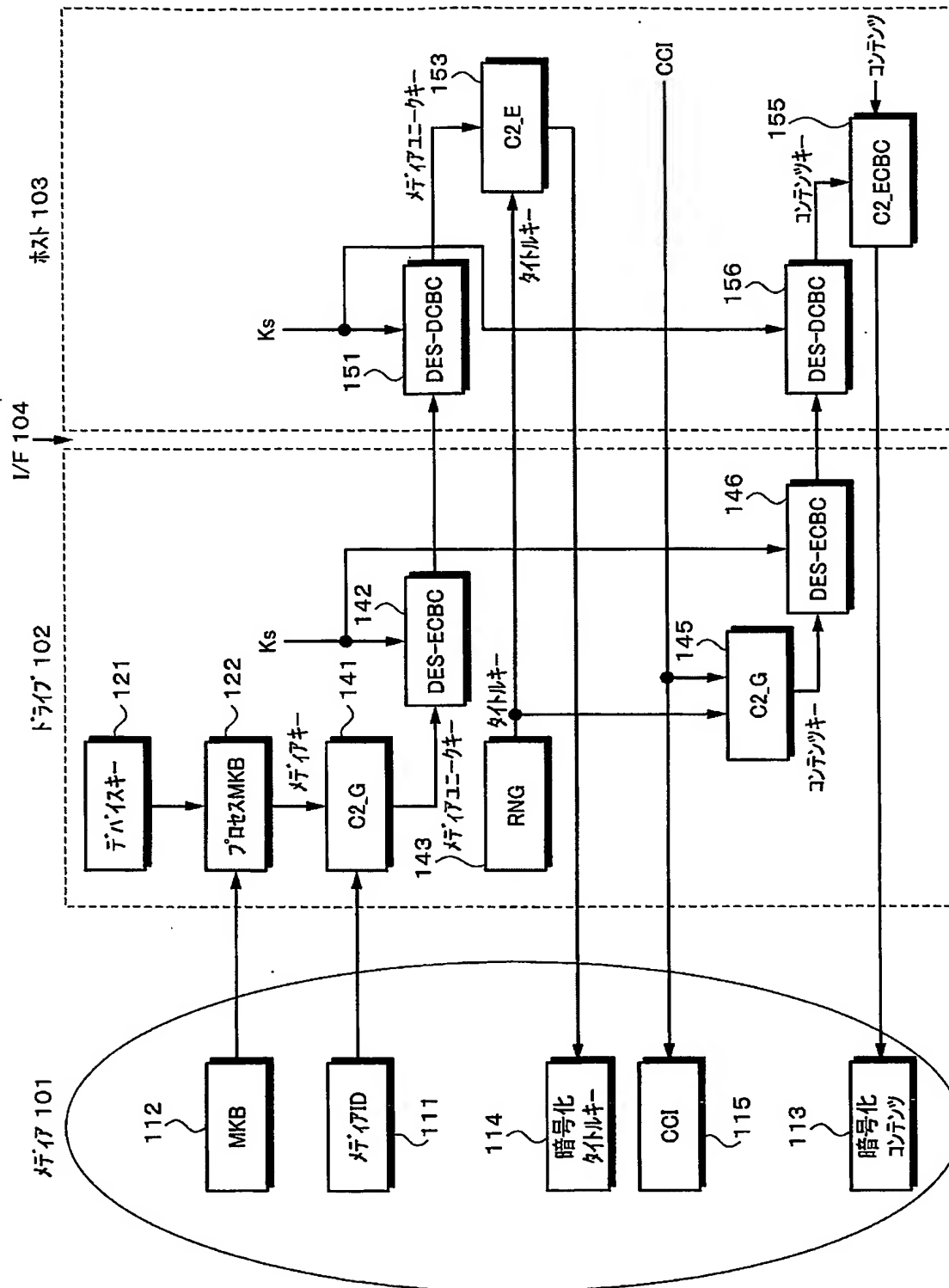
ドライブ102



【図 7】

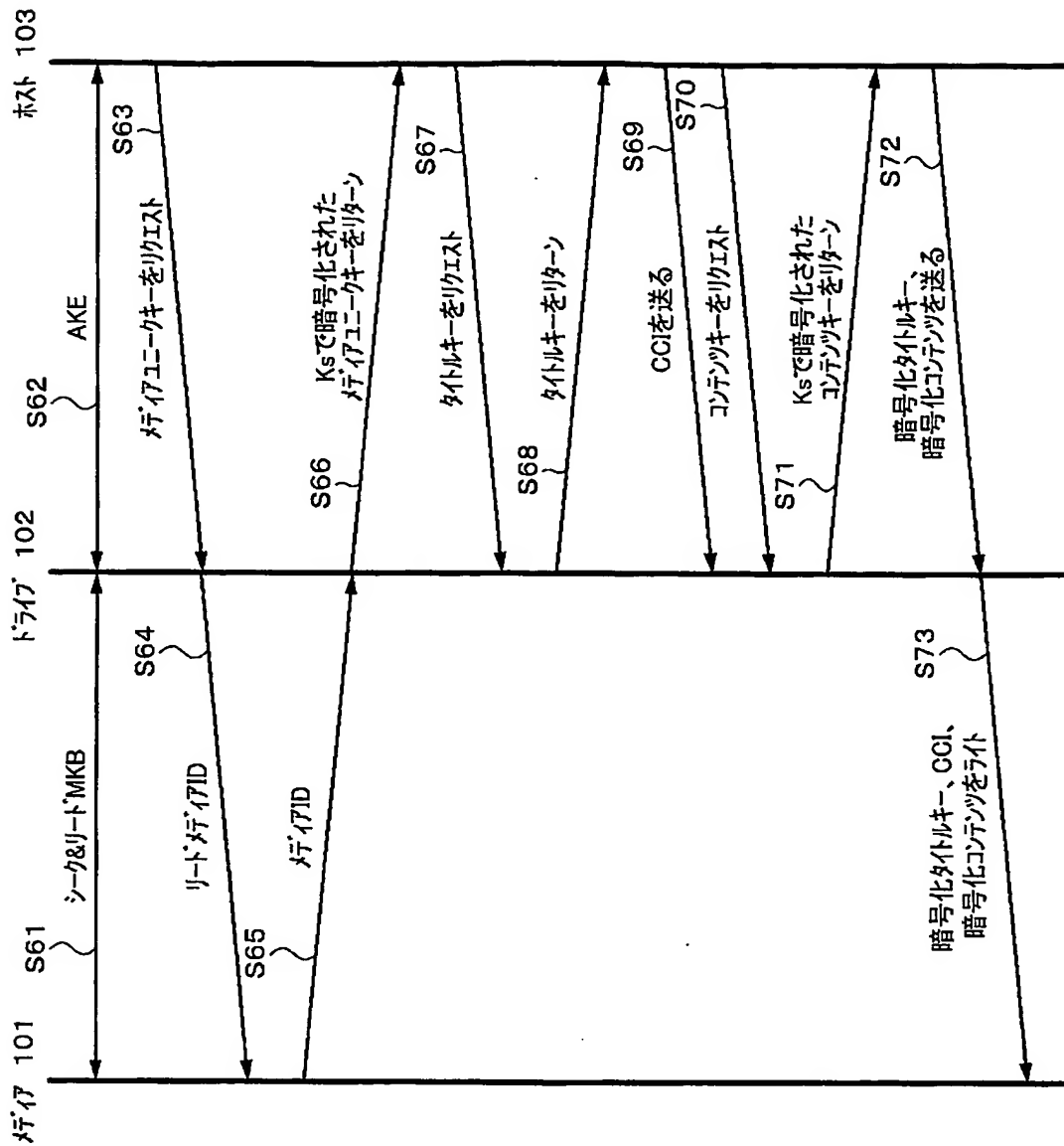


【图 8】

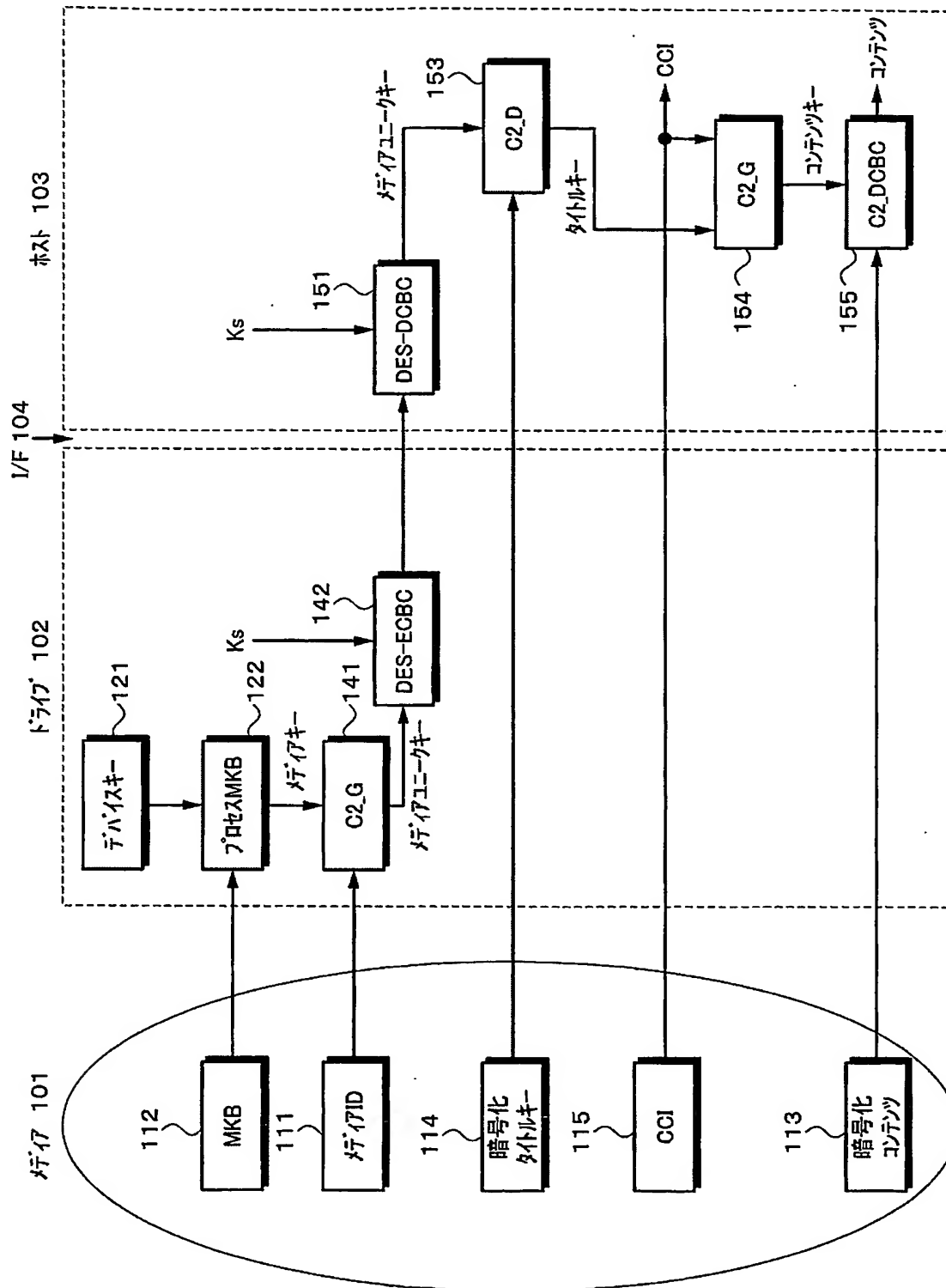




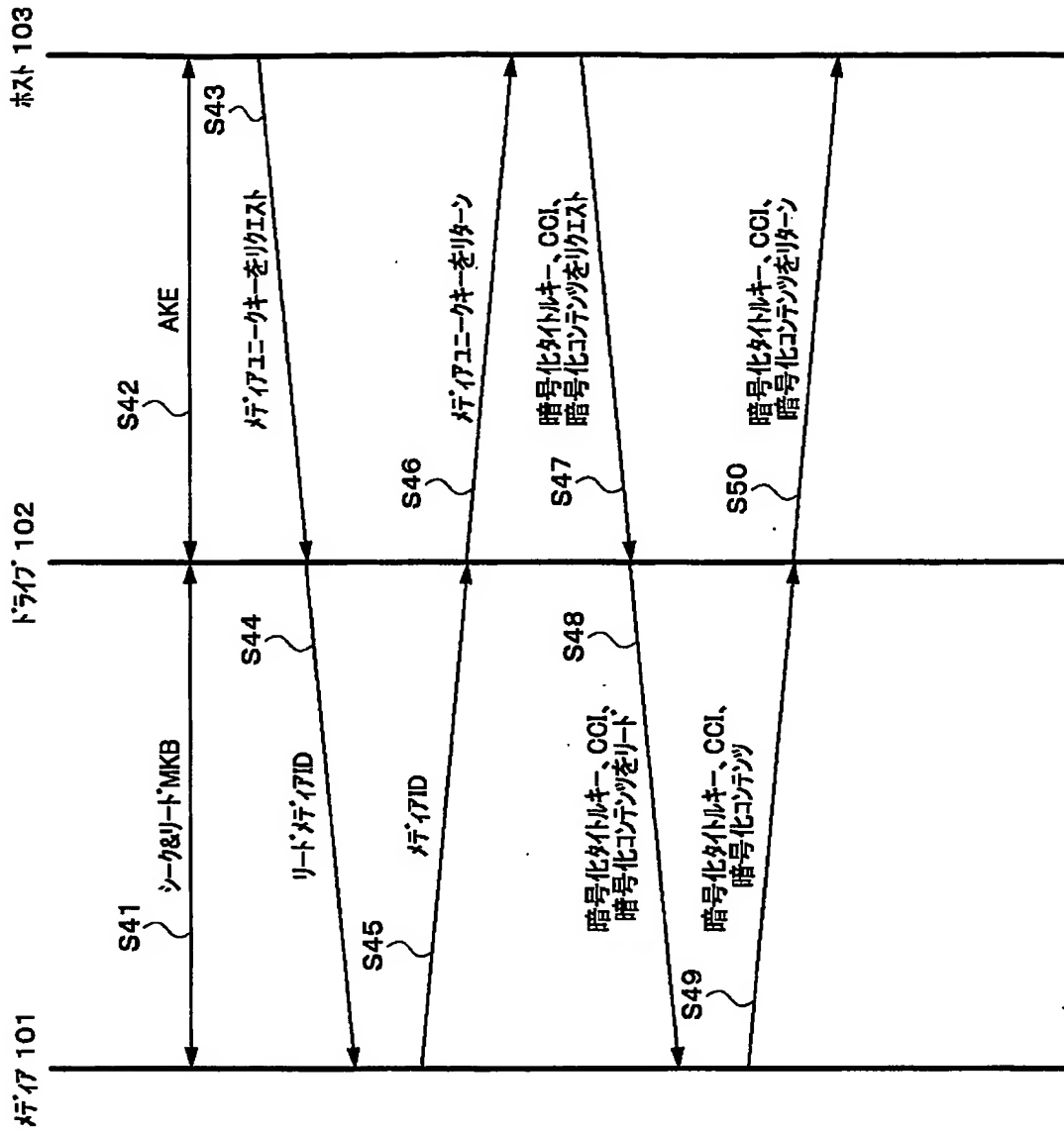
【図 9】



【図 10】



【図 11】



【書類名】 要約書

【要約】

【課題】 著作権保護技術の安全性を確保する。

【解決手段】 相互認証を行うドライブ102とホスト103とからレコーダが構成される。ドライブ102のC2\_\_G2141がメディアIDとメディアキーから計算したメディアユニークキーが相互認証によって生成したセッションキーKsを用いて暗号化されてからホスト103に転送される。ドライブ102の乱数発生器143が発生したタイトルキーがホスト103に転送される。ドライブ102のC2\_\_G2145がタイトルキーとCCIとから計算したコンテンツキーがセッションキーKsを用いて暗号化されてからホスト103へ転送される。ホスト103が復号したコンテンツキーを用いてコンテンツを暗号化し、ドライブ102が暗号化コンテンツ、暗号化タイトルキーおよびCCIをメディア101へ記録する。

【選択図】 図8

願 2 0 0 3 - 0 0 6 9 1 6

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 1 8 5 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社